Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 45 (2012) 880 – 887

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Symposium on Safety Science and Technology

The importance of correct control valve fail-safe mode documentation in avoiding process incidents

Jan C A WINDHORST*

WEC INC. 83 Dobler Avenue, Red Deer, Alberta T4R 1X3 Canada

Abstract

Achieving and maintaining a safe state during abnormal situations is essential for the safety design and safe operation of process facilities. This applies first of all to process control valve loops. The selection of the different control loop components can become a bit complicated because there are several design options and at least two different signal-response actions per component. This is especially true for split-range control loops with exclusively sequenced control valves that operate in different control ranges. These valves will never be open simultaneously and their fail-safe position under loss of signal and loss of motive utility requires special design attention. If the design was flawed or was compromised during maintenance then the system can respond in an unexpected manner during certain operating modes. Such an unexpected response was a contributing factor to a recent incident in a heavy oil processing facility. It involved very large vessels and resulted in a loss of containment situation inside and near a building where more than 40 people were working. Quick operator intervention prevented worse from happening but some of the vessels needed to have their "fitness for service" reconfirmed.

Keywords: fail-safe position; reverse; direct; split range control; turnaround; maintenance

1. Introduction

Cyclic Steam Stimulation (CSS) and Steam Assisted Gravity Drainage (SAGD) are often the methods of choice for gathering heavy oil from deposits that cannot be developed economically by mining. The steam application reduces the viscosity of the bituminous oil, allowing it to flow into collection holes of the producing wells. These holes are created by directional drilling. Down-hole positive displacement pumps direct the accumulated hot oil and condensate emulsion to the well pads and from there to the production facilities.

Once the hot oil/condensate emulsion arrives at the production facilities it is firstly collected in the slug catchers where some sand, water and produced gas are removed. The emulsion subsequently is sent to the separators where it is separated into sand, water, oil and produced gas. The produced gas is utilized as a supplemental fuel gas for the steam generators, reducing the need for natural gas for the CSS and SAGD processes. Condensate is treated to remove oil and other contaminants and re-used as boiler feed water for the steam generators.

The oil coming from the separators is treated with an emulsion breaker liquid and mixed with diluent, a gasoline type material, before being directed to the electrostatic treaters. In the treaters the diluent bitumen mixture (or dilbit) is upgraded to meet pipeline specifications by removal of most of the remaining gas, sand and water.

The five vessels: Slug Catcher, Separator A, Separator B, Treater A and Treater B are fairly large vessels with volumes that vary from ~ 200 m^3 to ~ 500 m^3. For climatic reasons the vessels are partially enclosed by a large building; a schematic view of which is given in Fig. 1.

* Corresponding author. *E-mail address:* janwindh@telusplanet.net

1877-7058 © 2012 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2012.08.253

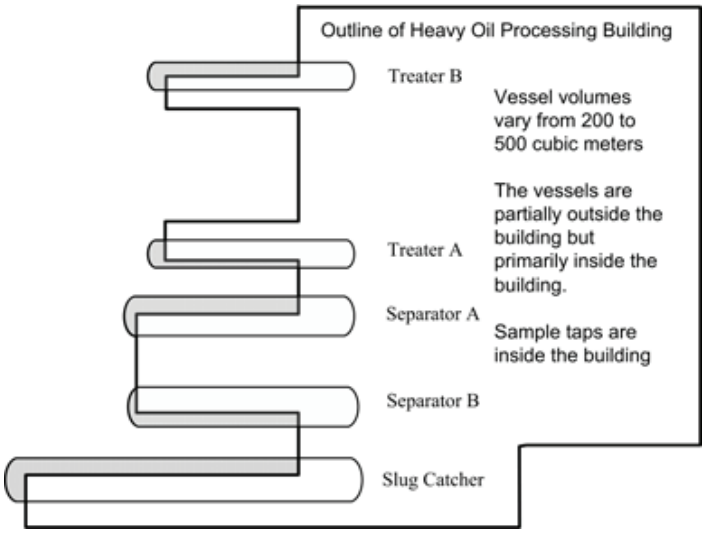


Fig. 1. Layout and housing scheme of the large heavy oil processing vessels.

2. Inherent process hazards

Water and steam based processes in cold climates are prone to freezing, which can result in equipment damage and in extreme cases to loss of process containment. In cold climates it is custom to place more equipment indoors than in warm climates; this is to limit freezing hazards and to facilitate or ease maintenance.High pressure and sub-atmospheric pressures (vacuum) are other conditions that can cause equipment damage unless the equipment was specifically designed for it. Vacuum can readily develop when steam condenses. These pressure extremes are often avoided through the installation of a split-range blanketing system where one controller controls two control valves (as shown in Fig. 2 and Fig. 3). The blanketing gas system sends make-up (fuel) gas to the vessels when they approach low pressure conditions and opens the vent valve to the produced gas header when vessel pressures approach unacceptable high levels. The split-range system is configured in such a way that the two control valves of the blanketing system cannot be open simultaneously.

It is difficult to pump heavy oilthrough pipelines because of its high viscosity; however, the addition of diluent, a naphtha type material, makes this possible(reduces the viscosity). The disadvantage of the diluent is its relatively low flash point, which introduces a new process hazard in the form of a vapour cloud explosion and flash fire potential.

Furthermore, the combination of indoor operations (see Fig. 1) and the use of fuel gas and the diluent can create conditions that are conducive for confined gas/vapour explosions upon a loss of process containment inside the building.

3. The incident

Besides the aforementioned inherent process hazards, these facilities are also exposed to additional hazards; e.g., hazards that are associated with the design of the facility. Such a hazard, specifically a high pressure situation, developed recently in a heavy oil facility that is similar to the one described in the introduction, causing a major incident. The incident took place during a turnaround (a maintenance shutdown) with a tight schedule.

3.1. The turnaround plan

The turnaround'sscope of work included: vessel maintenance and inspections, flare stack repairs and a Distributive Control System (DCS) upgrade. The original plan was to do the turnaround in the following order (see Figure-2 and Figure-3 for the equipment arrangements):

(1) isolate, clean and inspect the two separators and the two treaters with a "life" flare; i.e., the flare would be available to depressurize the vessels;

(2) isolate, clean and inspect the common slug catcher and smaller vessels with a "life" flare;

(3) shut down the flare and execute the flare stack repair work; and

(4) perform the (DCS) upgrade.

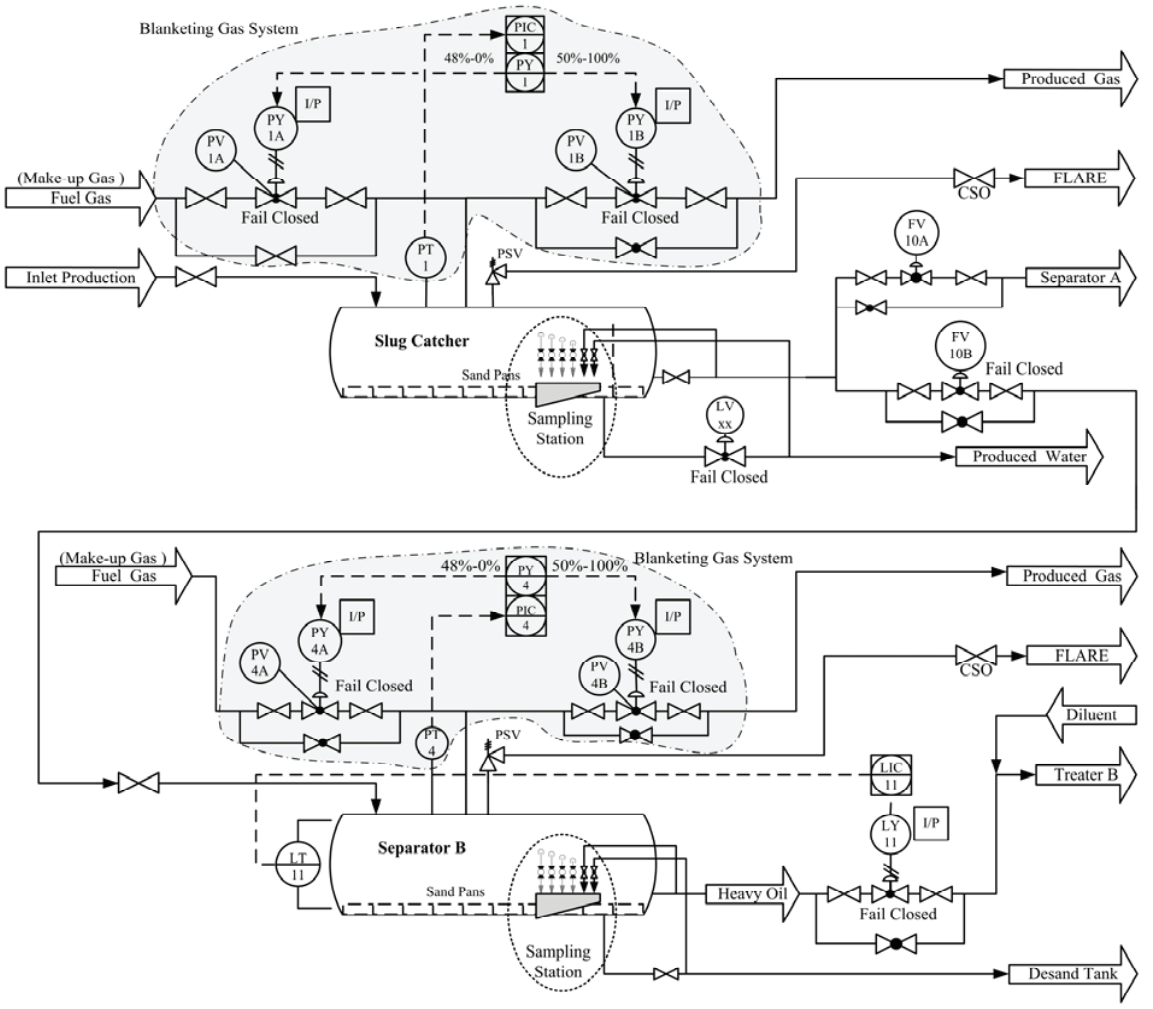


Fig. 2. Split range pressure control systems at front end of the heavy oil facility.

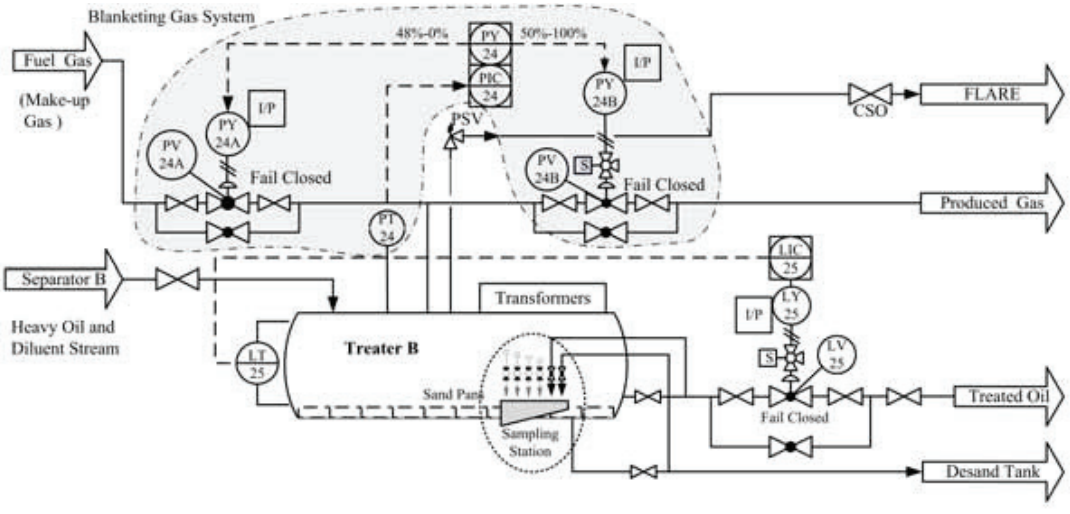


Fig. 3. A split range pressure control system at a treater vessel of the heavy oil facility.

3.2. Schedule compression

In order to limit the total downtime and resume partial production early on; it was decided to start with work on Separator A and Treater A and move the flare work forward. This would make it possible to resume partial production using the Separator A and Treater A vessels while work on Separator B and Treater B was being completed. The new schedule required the flare to be shut down after Treater A had been isolated, depressurized and cleaned.

The schedule change would make the flare temporarily unavailable for depressurizing the Slug Catcher, Separator A, Separator B and Treater B after their isolation. Venting the vessels to atmosphere was not an option because of the hydrogen sulfide content in the gas phase. The four vessels would therefore be isolated from the liquid process flows only and be left connected to the make-up (fuel) gas system. In this way the make-up gas would protect the four vessels against vacuum conditions as they cooled. A similar turnaround,on another heavy oil processing unit, had been successfully conducted several weeks earlier. However, for the unit under consideration, the DCS control of the make-up gas system would only be temporarily available, as the DCS needed to be shut down for the upgrade.

The fact that all DCS control functions and displays might not be available for up to 48 hours was recognized by the turnaround team but considered to be acceptable. The DCS unavailability was a concern to Plant Operations. Several times they requested information about how the processing unit would behave in the absence of DCS controls. However, they were not able to make a strong enough case,or able to convince the turnaround team, to have the turnaround schedule changed.

3.3. The turnaround

The sequence of events was as follows.

- Treater A was isolated, cleaned as planned and left isolated in preparation for work on the flare.
- The vent valves of the blanketing gas systems were isolated; i.e., no more gas was going to the produced gas header.
- The “Car Seal Open” (CSO) seals were removed from the stop valves downstream of the Pressure Safety Valves (PSVs) on the Slug Catcher, Separator A, Separator B and Treater B.
- Over the next nine hours gas pressures rose slowly in both separators. Initially, this caused the DCS to close the (blanketing) make-up gas control valves. However, the pressure kept on rising, eventually triggering visible and audible alarms in the control room. It is believed that, because of the high fuel gas header pressure (>60 bar-g), the control valves could not provide a tight shut-offand fuel gas was leaking into the separators. The alarms discredited the work plan that was based on the expectation that vessels pressureswould come down because of cooling. The next steps of the turnaround plan were nevertheless implemented.
- The DCS was shut down for the upgrade; this effectively silenced the ongoing high pressure alarms on the separators.
- Loss of the DCS power caused the make-up gas control inlet valves to the Slug Catcher, Separator A, Separator B and Treater B to open fully. This created a non-controllable path between the supply header with an operating pressure of more than 60 bar-g and the vessels which had been designed for less than 10 bar-g pressure.The fact that the valves assumed a “fail-open” position was a second unexpected event because the P&ID indicated a “fail-closed” default position for the make-up valves.
- There were several indicators that something was wrong; e.g., operators heard gas “screaming” through lines and “popping” sounds from PSV piping. In addition there was vapour leaking from a sealed man-way cover of the Slug Catcher.
- An operator manually closed the valves to the slug catcher’s make-up gas supply.
- Turnaround personnel, approximately 40, were evacuated from near the Slug Catcher and the gas trapped in the vessel was vented through a sample tap inside the building.
- Make-up gas valves on Separators A and B and Treater B were closed.
- The pressure of the make-up gas header, which had dropped, started to increase after the last vessel was isolated.
- After all non-emergency personnel had been evacuated; operators depressurized the vessels by opening sample valves. They also turned on the sample box exhaust fan on each of the vessels.
- A combustible gas analyzer that was under control of a programmable logic controller (PLC), and therefore independent of the (non-functional) DCS, triggered a “Lower Flammable Limit (LFL) exceeded” alarm in the control room.
- More than an hour later this “LFL” alarm cleared.

4. Blanketing system controls

An industrial control system typically consists of three parts (compare the blanketing gas system on the Slug Catcher in Fig. 2):

- a sensor system that converts a process variable into a suitable electrical signal (the measured Process Variable or PV),
- a controller that compares the signal against a desired value (the setpoint); where needed the controller initiates corrective action by sending a signal (the Manipulated Variable or MV) to the final element.
- a final element, usually a valve that is manipulated by the controller.

As shown in Fig. 2, the pressure transmitter PT1 sends an electric signal (identified by the dashed line - - - -) to the pressure controller PIC1, which in turn sends an electric signal to PY1A and PY1B. Usually both the PV and the MV are (different) 4-20 mA signals. PY1A and PY1B are current-to-pressure converter (aka I/P transducers), which translate the 4-20 mA control signal into a pneumatic (e.g., 3-15 PSIG) control signal.

A control valve's primary operation involves the positioning of the valve's movable part; e.g., its plug, relative to the stationary seat of the valve. The purpose of the valve's actuator is to accurately locate the valve plug in a position dictated by the control signal.

A secondary operation of a control valve can be, and often is, driving the valve's movable part to a safe position in case of a process upset. Control valves almost never provide tight shutoff because of the differential pressure across the plug. Driving a process to a safe position should, of course, be the task of a dedicated safety valve that can provide features such as a tight shut-off where needed.

Valves and actuators can be either reverse or direct-acting. In case of valves with up and down stem movement, reverse action means that the valve will open when the stem is pushed down while direct action means that lifting the stem will open the valve (see Fig. 4)[1-2]. For the actuators, reverse action means that the spring will extend the actuator stem while direct action results in the spring retracting the actuator stem (see Fig. 5[3]).

The combination of reverse and direct-acting valves and actuators results in four different combinations; these and the resulting valve/actuator functionality upon instrument air failure are shown in Table 1.

A typical control loop's number of design configurations is not limited to the air pressure and valve/actuator combinations shown in Table-1. Other configuration possibilities can be introduced by the transmitter, the controller, I/P transducers, etc.

The P&IDs indicated that the "fail-safe"position for both the make-up and the vent valve in the blanketing gas system was"fail- closed" or "FC".

From Table-1 it can be seen that this will require either a direct/reverse or a reverse/direct valve/actuator combination with respect to instrument air failure. In order to make it as "fail-safe" as possible; the most likely failure modes of other utilities have to drive the make-up and vent valves to the same"fail-closed" position. The most likely other failure mode will be a discontinuity in an electrical system, causing a low current (0 mA) fault.

The heavy oil processing plant's split range control system was originally configured to avoid vacuum conditions and overpressure conditions in the pressure vessels. Such ablanketing gas pressure control scheme is visualized in Fig. 6.

Assuming direct pressure transmitter signal proportionality; it can be seen that the relationship between the pressure transmitter and the vent valve is direct. As the process pressure increases, the direct acting controller supplies a larger signal to the vent valve and eventually opens it completely at the 100% controller output range. A controller failure that drives the controller output to 0 mA will close the vent valve.

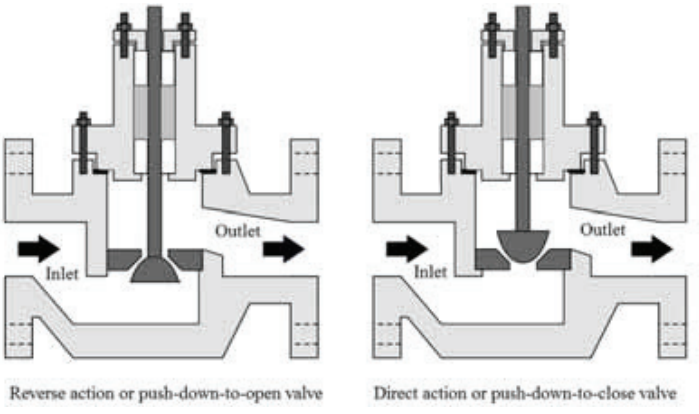
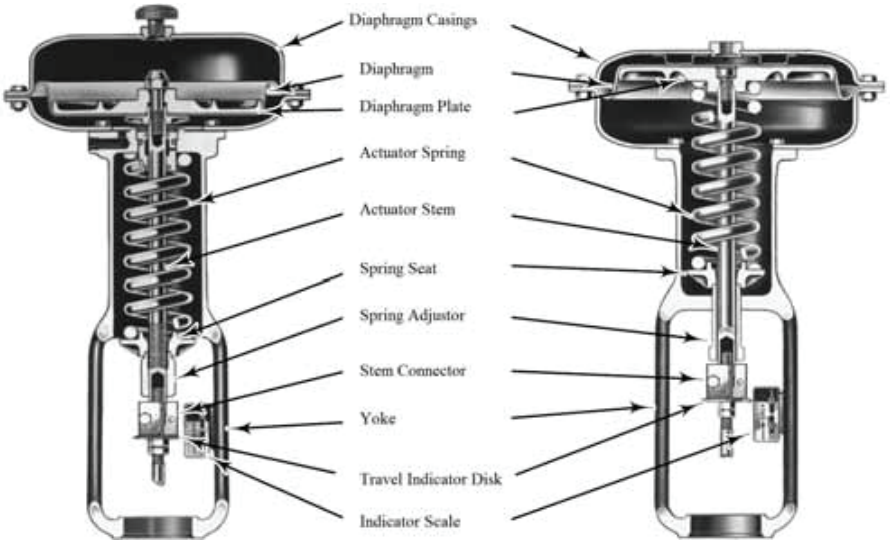


Fig. 4. Reverse-acting and direct-acting valves.



Reverse-Acting Actuator Direct-Acting Actuator

A reverse action actuator uses air to retract the actuator stem and its spring to extend the stem while the direct action actuator uses air to extend its stem and the spring to retract it. A direct action actuator provides fail-open action for push-down-to-close valves and fail-closed action for push-down-to-open valves.

Fig. 5. Reverse-acting and direct-acting actuators.

Table 1. Reverse and direct action valve/actuator combinations and system functionality upon instrument air failure.

	Actuator action: Reverse	Actuator action: Direct
Valve action: Reverse	Reverse/Reverse Valve opens upon air failure	Reverse/Direct Valve closes upon air failure
Valve action: Direct	Direct/Reverse Valve closes upon air failure	Direct/Direct Valve opens upon air failure

The relationship between the transmitter and the fuel gas valve is reverse. Without additional engineering measures a failure that drives the controller output to 0 mA will open the fuel gas valve completely. This makes the failure positions for loss of signal inconsistent with that of loss of air and creates a covert hazard that can materialize during enabling operating conditions, as happened at the heavy oil processing facility. A controller with sequenced 4-20 mA output signals can be used to correct the anomaly as shown in Fig. 7.

The fact that the make-up gas valves had different fail-safe positions for the “loss of instrument air” and the “loss of signal” failure modes, at the time of the incident, does not prove that the original design was wrong. Some staff members were not aware that this can occur and the error might have been introduced during an earlier turnaround or repair work.

5. API 579

The pressure ratio between the make-up gas header’s normal operating pressure and the Maximum Allowable Working Pressure (MAWP) of the exposed vessels was greater than 6[4]. This is far greater than the ASME VIII DIV 1 tensile strength factor of safetyof 3.5and constitutes a potential rupture situation[5]. Determining the exact pressures to which the vessels had been exposed was not possible because the DCS was down. However, pressure gauges were found that were stuck beyond their 11 bar maximum dial indication, nozzles on vessels had moved,and there had been loss of process containment conditions.

Therefore it is reasonable and prudent to state that the process vessels and their ancillary piping had been subjected to overpressures, which were well in excess of code requirements. It became therefore necessary to re-assess the vessels in accordance with API Standard 579-1/ASME FFSfor “Fitness-For-Service”.The assessment involved out-of-roundness assessments, detailed Finite Element (FE) analysis, and (re)hydro-test(s) with acoustic emission monitoring. Based on the analytical results, a successful hydro-test, and the goodmaterial properties, the equipment was considered fit for service.

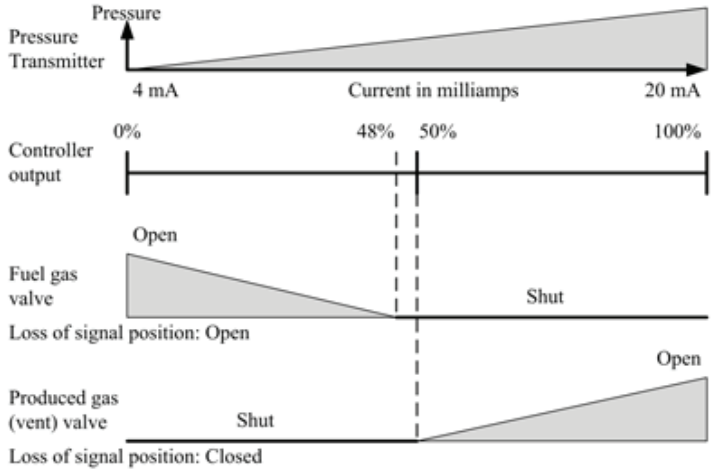


Fig. 6. Heavy oil processing vessel blanketing split range controls where the controller output drives identical 4-20 mA signals.

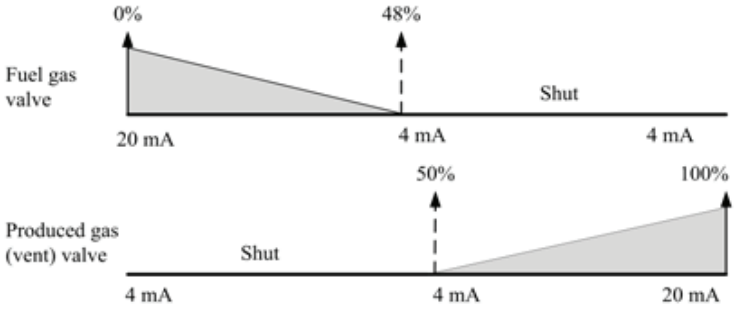


Fig. 7. Heavy oil processing vessel blanketing split range controls where the controller output drives exclusively sequenced 4-20 mA signals.

6. Discussion

The turnaround practices were inconsistent with good risk management practices. The rationale for this assertion lies in the fact that:

(1) the turnaround schedule had been compressed in order to resume production early on; and

(2) the turnaround involved unprecedented activities in combination with a great number of people in and around the process building.

Moreover, Plant Operations' concerns about those unprecedented practices had not been addressed in a professional manner. The turnaround team should have taken responsibility for establishing that the risk associated with the obviously severe hazards was acceptable. Obvious hazards include internal building explosions, external Vapour Cloud Explosions (VCEs), and staff exposure to gases, containing undetermined amounts of hydrogen sulfide. A drawing review is deemed inadequate as a risk assessment tool without input from different professional disciplines, specifically instrument and process safety engineering.

This was a "near-miss" incident, with respect to safety, that was possibly temporarily mitigated by the large size of the vessels and the small-size of the make-up valves and fuel gas header. The initial pressure ratio between the make-up gas header's normal operating pressure and the exposed vessels' MAWP that was initially greater than 6 most likely dropped quickly during the transient of pressurizing the vessels.This, and the fact that the operators manually isolated the vessels quickly, circumvented a severe loss of containment or vessel rupture.

However, the operator intervention put the operators themselves at risk, a situation that companies try to avoid.

Enabling Factors and Findings:

- Management of change was deficient;
- Six piping connections suffered a loss of process containment;
- Some nozzles on vessels had been moved (one up to 32mm);

- Staff had been conditioned to consider vacuum conditions in pressure equipment as the main hazard, neglecting other hazards;
- The control-operated make-up gas input valves had been identified as “fail-closed” on the P&IDs. At the time of the incident; however, the loss of signal fail-safe position was not consistent with the loss of air failure mode;
- Operator training was deficient: Firstly, the DCS should not have been turned off after the high pressure alarms had come in. An opportunity to stop a hazardous event chain had been missed. Secondly, the documentation for the removal of the car-seals of the open stop valves downstream of the PSVs did not meet regulatory requirements. Thirdly, operators should not endanger their lives by engaging into high risk mitigating actions to salvage equipment, even when well-intended. Fourthly, there was a lack of understanding of the process dynamics as well as fundamental process safety information and an unwillingness to halt the turnaround.

7. Recommendations

- It is good practice to capture process safety information in a special safeguarding manual; this manual should cover all process safety decisions that are being made during the life of a facility.
- Schedule considerations cannot take priority over safety and proper safety reviews.
- Pressure interfaces with a high $|\text{upstream}/\text{downstream}|$ pressure ratio values should be positively isolated during turnarounds; e.g., by blinds or double block and bleeds.
- Fail-safe positions of split range control systems with exclusively sequenced control valves should be reviewed during pre-startup safety reviews (PSSRs) to ensure that the fail-safe positions for loss of air and loss of signal are consistent.
- Training of plant staff should include information about underlying basic engineering aspects.
- Training of all technical staff but specifically the training of board operators should spell out that alarms are not to be ignored.

References

[1] Kuphaldt, Tony R., 2012. Lessons In Industrial Instrumentation. http://openbookproject.net/books/socratic/sinst/.
[2] Murrill, Paul W., 2000. Fundamentals of Process Control Theory 3rd Edition. Published by the ISA (The International Society of Automation).
[3] Fisher657 Diaphragm Actuator Sizes 30-70 and 87; Instruction Manual, D100306X012.
[4] API Standard 579-1/ASME FFS-1, Fitness-For-Service, Second Edition, 2007.
[5] ASME Section VIII, Boiler and Pressure Vessel Code Division 1, 2010.